UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPL NO.	FILING OR 371 (c) DATE	ART UNIT	FIL FEE REC'D	ATTY.DOCKET NO	DRAWINGS	TOT CLMS	IND CLMS
10/516,966	07/29/2005	2131	1152	18394-009US1	3	24	2

CONFIRMATION NO. 3136

26221
FISH & RICHARDSON P.C.
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

FILING RECEIPT

OC000000016724136

Date Mailed: 08/10/2005

Receipt is acknowledged of this regular Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please mail to the Commissioner for Patents P.O. Box 1450 Alexandria Va 22313-1450. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).**

Applicant(s)

Jean-Claude Pailles, Epron, FRANCE;
Vincent Boutroux, Hermanville Sur Mer, FRANCE;

Power of Attorney: The patent practitioners associated with Customer Number **26221**.

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/FR03/01535 05/21/2003

Foreign Applications

FRANCE 02/06915 06/05/2002

Projected Publication Date: 11/17/2005

Non-Publication Request: No

Early Publication Request: No

Title

Method and system for verifying electronic signatures and microcircuit card for carrying out said method

Preliminary Class

380

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject

matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Office of Export Administration, Department of Commerce (15 CFR 370.10 (j)); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

TFW Receipt

Attorney's Docket No.: 18394-009US1 / RVL/BR60677US 05502

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Pailes et al.	Art Unit	: 2131
Serial No.	: 10/516,966	Examiner	: Unknown
Filed	: July 29, 2005	Conf. No.	: 3136
Title	: METHOD AND SYSTEM FOR CHECKING DIGITAL SIGNATURES AND CARD WITH MICROCIRCUIT FOR USING THE METHOD		

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR CORRECTED OFFICIAL FILING RECEIPT

Please correct the Filing Receipt for the above-referenced application to include the correct title "METHOD AND SYSTEM FOR CHECKING DIGITAL SIGNATURES AND CARD WITH MICROCIRCUIT FOR USING THE METHOD". The title change was addressed in a Preliminary Amendment filed with the Application on December 3, 2004. A copy of the Preliminary Amendment is enclosed for your convenience.

Please supply a corrected Filing Receipt to the undersigned with respect to this application. A copy of the original Filing Receipt showing the desired changes in red ink is also attached for your convenience.

No fee is believed to be due. If, however, there are any charges or credits, please apply them to Deposit Account No. 06-1050.

CERTIFICATE OF MAILING BY FIRST CLASS MAIL

I hereby certify under 37 CFR §1.8(a) that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage on the date indicated below and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

August 25, 2006
Date of Deposit

Cassie Chandler
Signature

Cassie Chandler
Typed or Printed Name of Person Signing Certificate

Respectfully submitted,

Date: 8/25/06

Mandy Jubang
Reg. No. 45,884

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21409996.doc

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : France Telecom
Serial No. : N/A
Filed : Herewith
Title : METHOD AND SYSTEM FOR VERIFYING ELECTRONIC SIGNATURES AND MICROCIRCUIT CARD FOR CARRYING OUT SAID METHOD

Art Unit : Unknown
Examiner : Unknown

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRELIMINARY AMENDMENT

Prior to examination, please amend the application as indicated on the following pages.

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Label No. EV 411823701 US

December 3, 2004
Date of Deposit

AMENDMENTS TO THE SPECIFICATION:

Please add the following centered title at page 1, line 1:

Method and System for Checking Digital Signatures and Card with Microcircuit for using the Method

Insert the following centered heading at page 1, after the title:

BACKGROUND

Please add the following centered heading at page 3, line 4:

SUMMARY

Please add the following centered heading at page 5, line 29:

BRIEF DESCRIPTION OF THE DRAWINGS

Please add the following centered heading at page 6, line 5:

DETAILED DESCRIPTION

Please delete the centered heading beginning at page 16, line 3, which starts with "METHOD AND SYSTEM..."

Please replace the paragraph beginning at page 5, line 27 with the following amended paragraph:

According to yet another particular feature of the invention, this process comprises a phase of inserting a root public key in the certificates table, this insertion phase being done by write processing controlled by a MAC calculated using a specific key in the microcircuit and only known to ~~a transmitting~~ an entity ~~in~~ having issued the microcircuit.

Please replace the abstract at page 16 with the following amended abstract:

To check a digital signature, using a microcircuit card ~~(53)~~, the microcircuit being designed to receive and to process requests to check digital signatures, the process comprises storing in a memory in the microcircuit ~~(53)~~ a certificates table ~~(5, 5')~~ containing digest forms of authorized public keys, and a phase ~~(2)~~ of checking a digital signature consisting of: receiving ~~(21)~~ by the microcircuit the digital signature ~~(Sig(Aip,M)~~ to be checked and a public key ~~(A1p)~~ corresponding to a private key that was used to generate the digital signature to be checked; calculating ~~(22)~~ a digest form ~~(Hash(A1p))~~ of the received public key, searching ~~(23)~~ for the calculated digest form of the public key in the certificates table ~~(5, 5')~~, and decrypting ~~(25)~~ the digital signature using the received public key if the calculated digest form of the public key is located in the certificates table.

AMENDMENTS TO THE CLAIMS:

This listing of claims replaces all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) ~~Method~~ A method for checking a digital signature, involving a microcircuit ~~(53) that can be connected~~ connectable to a data processing system ~~(51)~~, the microcircuit being designed to receive requests to check digital signatures from the data processing system, and to process these requests, a digital signature being generated using a private key only known to a signatory entity and associated with a public key,

~~characterized in that it includes~~ said method comprising a step of storing a certificates table ~~(5, 5')~~ containing a digest form of at least one public key in a memory in the microcircuit ~~(53)~~, and a phase ~~(2)~~ of checking a digital signature comprising steps ~~consisting~~ of:

[[-]] receiving ~~(21)~~ by the microcircuit ~~the~~ a digital signature ~~($Sig(Ai_p,M)$)~~ to be checked and a public key ~~($A1_p$)~~ in a pair of keys comprising a private key that was used to generate the digital signature to be checked,

[[-]] calculating ~~(22)~~ a digest form ~~($Hash(A1_p)$)~~ of the received public key, and searching ~~(23)~~ for the calculated digest form of the public key in the certificates table ~~(5, 5')~~, and

[[-]] decrypting ~~(25)~~ the digital signature using the received public key if the calculated digest form of the public key is located in the certificates table.

2. (Currently Amended) ~~Method~~ The method according to claim 1,

~~characterized in that it comprises~~ further comprising a phase ~~(1)~~ of inserting a public key ~~(B_p)~~ into the certificates table ~~(5, 5')~~, comprising steps ~~consisting~~ of:

[[-]] receiving ~~(10)~~ by the microcircuit ~~(53)~~ a certificate ~~(<R,B>)~~ of the public key ~~(B_p)~~ to be inserted in the certificates table, and a public key ~~(R_p)~~ from a certification entity that generated the certificate, the certificate comprising the public key to be added into the certificates table and a digital signature of the certification entity, generated using a private key belonging to a pair of keys including the public key of the certification entity,

[[-]] calculating ~~(11)~~ by the microcircuit a digest form ~~($Hash(R_p)$)~~ of the public key ~~(R_p)~~ received from the certification entity, and searching ~~(12)~~ for the calculated digest form of the public key in the certificates table,

[[-]] decrypting ~~(14)~~ the digital signature using the public key received from the certification entity if the calculated digest form of the public key is located in the table,

[[-]] extracting ~~(17)~~ the public key ~~(B_p)~~ to be inserted from the certificate if the decrypted digital signature is correct,

[[-]] calculating ~~(18)~~ a digest ~~(Hash(B_p))~~ of the public key ~~(B_p)~~ extracted from the certificate, and inserting ~~(19)~~ the calculated digest in the certificates table.

3. (Currently Amended) ~~Method~~The method according to claim 2,

~~characterized in that~~ wherein the phase ~~(1)~~ of inserting a public key ~~(B_p)~~ in the certificates table ~~(5, 5')~~ comprises ~~the insertion~~ a step of inserting in the certificates table of a pointer ~~(8)~~ to the digest of the public key ~~(R_p)~~ of the certification entity that issued the certificate ~~(<R,B>)~~ of the public key to be inserted, so as to define a certification tree in combination with the inserted digest of the public key.

4. (Currently Amended) ~~Method~~The method according to claim 3,

~~characterized in that it includes~~ further comprising a phase ~~(3)~~ of deleting a digest ~~(Hash(B_p))~~ of a public key ~~(B_p)~~ from the certificates table ~~(5, 5')~~, ~~consisting~~ comprising steps of deleting from the certificates table the digest of a public key to be removed ~~from the certificates table~~, and deleting from the certificates table all digests of public keys associated with a pointer ~~(8)~~ indicating the public key ~~(B_p)~~ to be removed, ~~from the certificates table~~.

5. (Currently Amended) ~~Method~~The method according to ~~one of claims~~ claim 2 ~~to 4~~,

~~characterized in that~~ wherein each public key digest entered into the certificates table ~~(5, 5')~~ is associated with a validity end date ~~(7)~~, ~~and in that~~ the phase ~~(1)~~ of inserting a public key ~~(B_p)~~ into the certificates table ~~also comprises~~ further comprising steps ~~consisting~~ of reading in a received certificate a validity end date of the public key to be inserted ~~in the received certificate~~ ~~(<R,B>)~~, and entering the validity end date of the public key ~~(B_p)~~ to be inserted into the certificates table, together with the digest of the public key to be inserted, if it is earlier than the validity end date of the public key ~~(R_p)~~ of the certification entity read in the certificates table.

6. (Currently Amended) ~~Method~~The method according to ~~one of claims~~ claim 2 ~~to 5~~,

~~characterized in that~~ wherein each digest of a public key entered in the certificates table ~~(5, 5')~~ is associated with a usage counter ~~(41)~~ that is incremented every time that a digital signature is checked using the public key, and ~~in that it includes~~ said method comprising deletion of a public key digest from the certificates table when the usage counter is zero and the number of empty locations in the certificates table is less than a predetermined threshold.

7. (Currently Amended) ~~Method~~The method according to ~~one of claims~~ claim 2 ~~to 6~~, ~~characterized in that~~ wherein each public key digest entered into the certificates table ~~(5, 5')~~ is associated with a usage counter ~~(41)~~ that is incremented every time that a digital signature is checked using the public key, ~~on~~ and with a last usage date ~~(42)~~ that is updated every time that the associated usage counter is incremented, ~~and in that when the number of empty locations in the certificates table is less than a predetermined threshold, it also includes~~ said method further comprising a step to select a digest of a public key to be deleted as a function of the corresponding associated values of the usage counter and the last usage date when the number of empty locations in the certificates table is less than a predetermined threshold.

8. (Currently Amended) ~~Method~~The method according to ~~one of claims~~ claim 1 ~~to 7~~, ~~characterized in that~~ wherein the microcircuit ~~(53)~~ uses a predefined hashing function to calculate the digest forms of the public keys.

9. (Currently Amended) ~~Method~~The method according to ~~one of claims~~ claim 1 ~~to 8~~, ~~characterized in that it comprises~~ further comprising a phase of inserting a root public key ~~(R_p)~~ in the certificates table ~~(5, 5')~~, this insertion phase being done by a write processing controlled by a MAC calculated using a specific key in the microcircuit ~~(53)~~ and only known to ~~a transmitting~~ an entity ~~in~~ having issued the microcircuit.

10. (Currently Amended) ~~Method~~The method according to ~~one of claims~~ claim 1 ~~to 9~~, ~~characterized in that~~ wherein the digest of a public key memorized in the certificates table ~~(5, 5')~~ is obtained by calculating a digest of the public key associated with other information such as the validity end date of the public key, identity information and serial numbers, this information being transmitted to the microcircuit ~~(53)~~ every time that the signature is checked using the public key.

11. (Currently Amended) ~~Method~~The method according to ~~one of claims~~ claim 1 ~~to 10~~, ~~characterized in that~~ wherein the digest of a public key memorized in the certificates table ~~(5, 5')~~ is obtained by calculating a digest of the certificate received by the microcircuit ~~(53)~~ when the public key is inserted in the certificates table, this certificate being transmitted to the microcircuit every time that the signature is checked using the public key.

12. (Currently Amended) ~~Method~~The method according to ~~one of claims~~ claim 1 ~~to 11~~, ~~characterized in that~~ wherein the certificates table ~~(5, 5')~~ is stored in a secure memory area in the microcircuit ~~(53)~~.

13. (Currently Amended) ~~Card provided with a~~ A microcircuit ~~(53), characterized in that it uses the method according to one of claims 1 to 12~~ designed to receive requests to check digital signatures from a data processing system, and to process these requests, a digital signature being generated using a private key only known to a signatory entity and associated with a public key, said microcircuit comprising:

memory means for storing a certificates table containing a digest form of at least one public key,

means for receiving a digital signature to be checked and a public key in a pair of keys comprising a private key that was used to generate the digital signature to be checked,

means for calculating a digest form of the received public key, and for searching for the calculated digest form of the public key in the certificates table, and

means for decrypting the digital signature using the received public key if the calculated digest form of the public key is located in the certificates table.

14. (Canceled)

15. (New) The microcircuit according to claim 13,

further comprising:

means for receiving a certificate of the public key to be inserted in the certificates table, and a public key from a certification entity that generated the certificate, the certificate comprising the public key to be added into the certificates table and a digital signature of the

certification entity, generated using a private key belonging to a pair of keys including the public key of the certification entity,

means for calculating a digest form of the public key received from the certification entity, and for searching for the calculated digest form of the public key in the certificates table,

means for decrypting the digital signature using the public key received from the certification entity if the calculated digest form of the public key is located in the table,

means for extracting the public key to be inserted from the certificate if the decrypted digital signature is correct,

means for calculating a digest of the public key extracted from the certificate, and for inserting the calculated digest in the certificates table.

16. (New) The microcircuit according to claim 15,

further comprising means for inserting in the certificates table a pointer to the digest of the public key of the certification entity that issued the certificate of the public key to be inserted, so as to define a certification tree in combination with the inserted digest of the public key.

17. (New) The microcircuit according to claim 16,

further comprising means for deleting from the certificates table a digest of a public key to be removed, and means for deleting from the certificates table all digests of public keys associated with a pointer indicating the public key to be removed.

18. (New) The microcircuit according to claim 15,

further comprising: means for reading in a received certificate a validity end date of a public key to be inserted, and means for entering the validity end date of the public key to be inserted into the certificates table, together with the digest of the public key to be inserted, if the validity end date is earlier than the validity end date of the public key of the certification entity read in the certificates table.

19. (New) The microcircuit according to claim 15,

further comprising means for incrementing a usage counter associated with each public key digest entered into the certificates table, every time that a digital signature is checked using the public key, and means for deleting a public key digest from the certificates table when the

associated usage counter is zero and the number of empty locations in the certificates table is less than a predetermined threshold.

20. (New)The microcircuit according to claim 19,

further comprising means for updating a last usage date associated with each public key digest entered into the certificates table, every time that a digital signature is checked using the public key, means for deleting a public key digest from the certificates table when the number of empty locations in the certificates table is less than a predetermined threshold, and means for selecting a digest of a public key to be deleted as a function of the corresponding associated values of the usage counter and the last usage date.

21. (New)The microcircuit according to claim 13,

further comprising means for executing a predefined hashing function to calculate the digest forms of the public keys.

22. (New)The method according to claim 13,

further comprising means for inserting a root public key in the certificates table, using a write processing controlled by a MAC calculated using a specific key in the microcircuit and only known to an entity having issued the microcircuit.

23. (New)The method according to claim 13,

wherein the means for calculating the digest of a public key memorized in the certificates table comprise means for calculating a digest of the public key associated with other information comprising the validity end date of the public key, identity information and serial numbers, this information being transmitted to the microcircuit every time that the signature is checked using the public key.

24. (New)The method according to claim 13,

wherein the means for calculating the digest of a public key memorized in the certificates table comprise means for calculating a digest of the certificate received by the microcircuit when the public key is inserted in the certificates table, this certificate being transmitted to the microcircuit every time that the signature is checked using the public key.

25. (New)The method according to claim 13, wherein the memory means for storing the certificates table is a secure memory area.

REMARKS

The applicant presents claims 1-13 to 15-25 for examination. Claims 1 and 13 are independent. Claim 14 has been canceled.

Entry hereof and early passage to issue are respectfully requested.

Please apply any fees associated with this Preliminary Amendment or the accompanying application, which have not already been covered by check, to Deposit Account 06-1050.

Respectfully submitted,

Date: 12/3/04

Mandy Jubang
Reg. No. 45,884

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906